UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with **tntgentlemansclub@icloud.com** that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014

Case No. 18-917M (NJ)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Wisconsin:

See Attachment A

I find that the affidavit(s) or any recorded testimony, establish probable cause to search and seize the person or property described above and that such search will reveal:

See Attachment B

YOU ARE COMMANDED to execute this warrant ON OR BEFORE September 25, 2018 *(not to exceed 14 days)*
☐ in the daytime between 6:00 a.m. and 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Nancy Joseph.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: September 11, 2018 3:00 pm

Judge's signature

City and State: Milwaukee, Wisconsin — Hon. Nancy Joseph, U.S. Magistrate Judge
Printed Name and Title

AO 93 (mod. 5/14) Search and Seizure Warrant

Return

Case No:	Date and time warrant executed:	Copy of warrant and inventory left with:
18-917 (M) (NJ)	09/11/2018 4:51 pm	Apple Privacy and LE Compliance

Inventory made in the presence of:

FE Kerry Koleckeck for processing Apple SW returns

Inventory of the property taken and/or name of any person(s) seized:

Apple provided iCloud results via email on 10/29/2018 at 6:29pm.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the undersigned judge.

Date: 3/4/2019

Executing officer's signature

Heather Wright / Special Agent

Printed name and title

Subscribed, sworn to, and returned before me this date:

Date: March 4, 2019

United States Magistrate Judge

ATTACHMENT A

Premises to be Searched

This warrant applies to information associated with **tntgentlemansclub@icloud.com** (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for the account listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

f. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

g. All records pertaining to the types of service used;

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government.

All information described above in Section I that constitutes evidence or instrumentalities of violations of Title 18, United States Code, Sections 1594(b) (conspiracy to engage in sex trafficking), 1952 (use of facility in interstate commerce to promote, manage, or carry on unlawful prostitution activity), or 1956 (money laundering), from 2012 to the present, including:

a. All information and communications in any form, including text messages, instant messages, emails, and other forms of messages concerning the operations of TNT Gentleman's Club, including the scheduling of dancers, nightly revenues at TNT, amounts that dancers had earned or were owed by TNT, negotiations with dancers' "handlers" or "pimps," and other club-related business, whether legal or illegal;

b. Photographs or videos of dancers or strippers, the interior or exterior of TNT, the staff of TNT, or any other image related to the operation of TNT;

c. All call and messaging logs;

d. Contact lists, to assist with the interpretation of the communications documented in the call logs and to identify the parties listed as affiliated with TNT;

e. Evidence of user attribution, showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, notes, documents and Internet browsing history;

f. Evidence of use of third-party apps and websites, such as Facebook, related to the offenses under investigation;

g. The identity and location of the persons who have used the Apple ID;

h. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

i. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information); and

j.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.Evidence that may identify any co-conspirators, aiders and abettors, or victims including records that help reveal their whereabou